PLIEGO DE PRESCRIPCIONES TÉCNICAS

Nº EXPEDIENTE: CH00-25-001

ACUERDO MARCO DE CIBERSEGURIDAD

ÍNDICE

1. ANTECEDENTES

Verificaciones Industriales de Andalucía S.A. (en lo sucesivo, VEIASA) es una sociedad mercantil del sector público andaluz, cuyo objeto social es la realización de las actuaciones de inspección y control reglamentarios derivadas de la aplicación de las distintas reglamentaciones agrícolas, industriales, mineras y energéticas que le sean asignadas por la Junta de Andalucía, así como la realización de todo tipo de trabajos, obras, estudios, informes, proyectos, dirección de obras, consultorías, asistencias técnicas y servicios públicos en estas materias, que le puedan ser atribuidas por la Administración competente, dentro o fuera del territorio nacional, con sujeción a la normativa vigente y particularmente a la relativa a la normativa referente a la defensa de la competencia; especialmente, es cometido de la Sociedad la gestión del Servicio Público de Inspección Técnica de Vehículos (ITV) y el control metrológico.

VEIASA, en su calidad de sociedad mercantil del sector público andaluz, en cuyo capital participa integra y únicamente la Junta de Andalucía, está incluida en el ámbito de aplicación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (LCSP, en lo sucesivo) en virtud de lo establecido en el artículo 3.1.h.

VEIASA como entidad del sector público andaluz, está obligada al cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, el ENS).

VEIASA dispone de certificación que acredita este cumplimiento para sistemas de categoría Media según el Anexo 1 del ENS.

Para mantener sus obligaciones de cumplimiento normativo, mejorar los niveles de seguridad de sus sistemas de información y de las infraestructuras que dan soporte a estos y, en consecuencia , incrementar la seguridad de los servicios que ofrece a la ciudadanía, VEIASA se plantea la contratación de los servicios descritos en el presente pliego.

2. OBJETO DEL ACUERDO MARCO

En el marco de las actividades del ciclo de mejora continua del Sistema de Gestión de la Seguridad de la Información de VEIASA, y con objeto de poder desarrollar las distintas

iniciativas en materia de ciberseguridad, la empresa necesita complementar su capacidad a través de servicios como los que son objeto del presente acuerdo marco.

En este ámbito, el presente pliego de prescripciones técnicas tiene por objeto establecer las condiciones técnicas que regirán la ejecución de un acuerdo marco que incluye servicios cuya finalidad es:

1. El refuerzo de la ciberseguridad en el ámbito de VEIASA, mediante la revisión y mejora continua de sus procesos y procedimientos, que contemplen entre otros la continuidad en la disponibilidad de los servicios que se prestan a la ciudadanía y el aseguramiento de la confidencialidad de la información.
2. El cumplimiento del Esquema Nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo) y de otra normativa de aplicación en los sistemas de VEIASA, garantizando el mismo mediante la validación por medio de auditorías internas de cumplimiento.
3. La evaluación y reducción del riesgo de que se materialice un incidente de seguridad y la mejora de las capacidades de prevención, detección y respuesta a incidentes
4. La concienciación y formación en materia de ciberseguridad como forma de prevención, tanto de forma general para todo su personal, como de forma especializada para los perfiles TIC que así lo requieran.
5. El fortalecimiento de la ciberseguridad a través de la renovación de infraestructuras críticas, la implementación de nuevas soluciones de seguridad avanzada, y un servicio continuo 24/7 para la monitorización y vigilancia continua para la detección y prevención de cualquier incidente de seguridad que pudiera materializarse.
6. Mejorar la protección y asegurar la efectividad de las medidas de seguridad desplegadas en los distintos sistemas de información de VEIASA, mediante la realización de análisis técnicos de ciberseguridad de los sistemas y de las infraestructuras que los soportan.
7. Mejorar la seguridad de los usuarios (ciudadanía, proveedores y personal propio) de los sistemas de información

3. DIVISIÓN EN LOTES

Los servicios solicitados en el presente Acuerdo Marco se clasifican en tres lotes diferenciados por el tipo de servicio:

- Lote 1 - Infraestructura de Seguridad Perimetral: Incluye equipamiento de seguridad perimetral, licencias relacionadas con el uso este equipamiento, actividades de soporte en su implantación y mantenimiento, así como licencias de herramientas de protección.

- Lote 2 - Monitorización y Vigilancia de la Ciberseguridad: incluye las tareas necesarias para la protección de la ciberseguridad a través de la prestación de servicios de prevención, protección, detección y respuesta.

- Lote 3 – Asistencia Técnica y de Cumplimiento Normativo en Ciberseguridad: apoyo al gobierno de la seguridad, al análisis y gestión de riesgos y cumplimiento normativo (GRC), auditorías técnicas de seguridad y actividades de formación y concienciación en ciberseguridad.

Cada contrato basado, por su parte, detallará y concretará los elementos de gestión, los volúmenes (o nivel de actividad) y el plazo requerido para el objeto que se pida. También detallará las actividades específicas a realizar por parte de los adjudicatarios, así como los requisitos, entregables o hitos establecidos.

4. DESCRIPCIÓN DE LOS SERVICIOS REQUERIDOS

VEIASA proporcionará a los licitadores (Anexo I del PPT), un documento detallado con todos los sistemas preexistentes, su arquitectura y los niveles de criticidad a los efectos de su integración con la solución propuesta.

Este anexo es de carácter confidencial, por lo que será remitido al licitador previa solicitud al correo licitaciones@veiasa.es, debiendo aportar en dicha solicitud la Cláusula de Confidencialidad (Anexo II del PPT) debidamente cumplimentada, firmada y sellada por representante con poder suficiente (debiendo acreditarse igualmente el poder de representación).

4.1. LOTE 1: INFRAESTRUCTURA DE SEGURIDAD PERIMETRAL

4.1.1. Objeto

El objeto de este lote, es la mejora de la seguridad de las infraestructura de seguridad perimetral de VEIASA.

4.1.2. Actividades a desarrollar y suministro de equipamiento

Instalación y configuración de firewalls de última generación, incluyendo la provisión de licencias, operación y mantenimiento de los siguientes elementos:

- Licencias Firewall CPD (Centro de Procesamiento de Datos): Equipos diseñados para la protección avanzada de los centros de procesamiento de datos de VEIASA, garantizando la seguridad de los sistemas críticos.
- Licencias Firewall 1600 y 1570: Equipos destinados a proporcionar seguridad perimetral en las oficinas y otras sedes de VEIASA.
- Licencia Consola: Herramienta de gestión centralizada para los firewalls, permitiendo la administración de las políticas de seguridad, generación de logs y análisis en tiempo real.
- Licencias e integración de soluciones de seguridad Sandbox, ZTNA, y WAAP para la protección integral de la infraestructura.
- Operación y mantenimiento: Servicio continuo de soporte y asistencia técnica para garantizar que los firewalls están actualizados y operativos en todo momento, incluyendo:

  - Monitorización y soporte a incidencias.
  - Aplicación de parches de seguridad.
- Servicios Adicionales:
  - Implantación de firewalls adicionales en localizaciones clave.
  - Revisión y ajuste periódico de las políticas de seguridad de red para garantizar la adecuación a las amenazas emergentes.
- Informes de seguimiento de operación y mantenimiento.

4.1.2.1. Suministro de Ciberseguridad en Infraestructura Hiperconvergente

A continuación se detalla la adquisición de equipamiento de seguridad perimetral para su integración en una solución hiperconvergente basada en una infraestructura de nube híbrida.

El suministro de los siguientes elementos de infraestructura de Check Point está sujeto a requerimientos de throughput y renovación tecnológica.

La inclusión de estos elementos permite garantizar una protección avanzada y un rendimiento óptimo en entornos empresariales críticos.

- Firewalls Adicionales - Modelo Check Point 1600 Next-Gen Firewall (4 unidades). Características principales:
  - Seguridad avanzada con prevención de amenazas en tiempo real.
  - Soporte para VPN, IPS, Antivirus, Anti-Bot y más.
  - Capacidad de throughput optimizado para pequeñas y medianas empresas (SMB) y oficinas remotas.
- SFP+ Transceiver 10G - Modelo: Check Point CPAC-TR-10SR-SSM (4 unidades). Características principales:
  - Módulo transceptor SFP+ de 10Gbps.
  - Compatible con los modelos 1600 para expansión de red.
  - Facilita la conectividad de alta velocidad en entornos de firewall.
- Firewalls Adicionales Modelo: Check Point 1800 Next-Gen Firewall (4 unidades). Características principales:
  - Protección mejorada para entornos empresariales de alto rendimiento.
  - Soporta administración centralizada con Check Point SmartConsole.
  - Alto rendimiento para redes con altos requerimientos de seguridad y throughput.
- QSFP28 Transceiver 100G (4 unidades) Modelo: Check Point CPAC-TR-100SR-SSM. Características principales:
  - Módulo transceptor QSFP28 de 100Gbps.
  - Compatible con modelos 1800 y otros dispositivos de Check Point.
  - Ideal para conexiones de backbone de alta velocidad en centros de datos.

4.1.2.2. Licencias Firewall CPD

Para los Servicios Centrales de VEAISA se requiere la renovación anual de los soportes y licencias de 2 equipos Check Point modelo SG-16200. El soporte y licencias serán del siguiente nivel:

- Soporte: soporte directo con el fabricante tipo 24x7
- Licencias:
    - Prevención de amenazas de nueva generación: Capacidad de albergar distintos tipos de servicios de seguridad de manera combinada: firewall, soporte nativo de reglas de nivel 7, identificación y control de aplicaciones y de contenido, filtrado web (bloqueando acceso a páginas inapropiadas y/o peligrosas), reconocimiento y gestión de identidades, sistemas de protección de intrusión (IPS), seguridad DNS, antibot, antispam, antimalware y zero phishing
    - Prevención y mitigación de amenazas de día cero: capacidad de realizar diagnósticos de ficheros y extracción de contenido malicioso en emuladores Sandbox.

4.1.2.3. Licencias Firewall 1600 y 1570

Para las estaciones de Inspección Técnica de Vehículos (estaciones de ITV) se requiere la renovación anual de los soportes y licencias de 80 equipos Check Point modelo SG-1570 y 62 equipos Check Point SG-1600. El soporte y licencias serán del siguiente nivel:

- Soporte: soporte directo con el fabricante tipo 24x7
- Licencias:
    - Prevención de amenazas de nueva generación: Capacidad de albergar distintos tipos de servicios de seguridad de manera combinada: firewall, soporte nativo de reglas de nivel 7, identificación y control de aplicaciones y de contenido, filtrado web (bloqueando acceso a páginas inapropiadas y/o peligrosas), reconocimiento y gestión de identidades, sistemas de protección de intrusión (IPS), seguridad DNS, antibot, antispam, antimalware y zero phising

4.1.2.4. Licencias de consola para administración de los Firewalls, log y reporting

Sera necesario renovar anualmente los soportes y las licencias de la actual consola de gestión, configuración y administración tanto de los equipos como de los logs, eventos y alertas de seguridad generados por la planta firewalls de VEIASA.

La consola estará preparada para tener una almacenar un volumen de logs de 100GB diarios con una retención de al menos 3 meses. Así mismo, dispondrá de las licencia necesarias para exportar 5GB de logs al día.

Tendrán las licencias necesarias para:

- Realizar informes personalizables que den visibilidad completa de las amenazas detectadas, riesgos de seguridad, tipología de tráfico cursado en la red, etc.

- Herramienta de gestión y correlación para automatizar la agregación y la correlación de los datos de registro, y los patrones de ataque potenciales, facilitando a los técnicos de VEIASA la revisión de logs para que puedan identificar rápidamente las amenazas de seguridad reales.

La consola tendrá la posibilidad de gestionarse desde un portal único de administración junto al resto de soluciones incluidas en el lote 1 del expediente.

La consola dispondrá de licencias necesarias para gestionar como mínimo 144 firewalls y contará con soporte directo con el fabricante tipo 24x7.

4.1.2.5. Licencias de ZTNA

Se requiere una solución de acceso seguro a los recursos corporativos de VEIASA tipo Zero Trust para un total de 50 usuarios. La solución deberá poseer las siguientes características:

- La solución ofertada debe ser entregada como una solución SaaS y con un único portal de administración junto al resto de soluciones incluidas en el lote 1 del expediente
- Deberá combinar las protecciones en el dispositivo y en la nube para ofrecer una experiencia de usuario mejorada.
- La solución permitirá el acceso remoto a usuario a aplicaciones HTTP/HTTPS, VNC y SSH sin necesidad de instalar agente en los dispositivos desde el que se accede.
- La solución deberá conectarse con data centers privados locales y data centers públicos
- Diversidad geográfica en los puntos de presencias (PoPs). La solución deberá de tener al menos 2 PoPs en España.
- Debe proporcionar una conectividad de Red Privada Completa:
  - La solución debe permitir la conectividad completa en malla completa en cualquier dirección del tráfico, facilitando el acceso entre CPDs, sedes y usuarios. Dicha Red Full Mesh debe estar incluida sin licencia adicional
  - La solución debe ofrecer redundancia con soporte para túneles redundantes a zonas de disponibilidad o regiones separadas.
  - Debe permitir crear varías redes independientes desde el mismo portal de gestión
- La solución debe proporcionar protección DNS integrada que proteja a los usuarios contra los ataques de suplantación de DNS. La seguridad DNS debe verificar que las direcciones IP de los sitios web son correctas antes de que los usuarios se conecten a ellos.
- La solución debe permitir la instalación de un agente ligero en el dispositivo final. Esto no debe requerir ningún hardware o instalación local de VM. El agente debe realizar la inspección SSL en el dispositivo.
- La solución debe proteger el tráfico de los usuarios, incluso cuando no estén conectados a la red corporativa.
- La solución debe proteger el tráfico desviado (Split tunneling), incluyendo opciones de inclusión/exclusión y compatibilidad con IP y FQDN.

- La solución no debe descifrar el tráfico fuera del dispositivo del usuario
- La solución debe permitir una configuración flexible de las políticas
- La solución debe permitir múltiples despliegues de red con políticas específicas para cada red
- La solución debe proporcionar direcciones IP estáticas privadas para cada cliente
- La solución debe soportar el uso de túneles IPSec para conectar recursos corporativos

Postura de seguridad de los dispositivos

- Debe permitirle realizar comprobaciones de la postura de los dispositivos para garantizar que sólo puedan acceder a su red aquellos que cumplan determinadas condiciones de seguridad
- Debe añadir una capa adicional de seguridad verificando la "postura" o el estado de seguridad de un dispositivo antes de que pueda acceder a aplicaciones o datos. Estas verificaciones podrán realizarse antes de una conexión o de forma continuada cada 20 minutos
- Los administradores deben permitir el acceso a la red sólo desde dispositivos que cumplan una o más de las siguientes políticas:
    - presencia de un software antivirus específico en el dispositivo
    - presencia de un archivo específico en el dispositivo
    - Si el almacenamiento del dispositivo está cifrado
    - Si el dispositivo dispone de un certificado específico
    - Si hay un determinado proceso en ejecución
    - Registro: Verificará una clave de registro específica. (Ejemplo: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\NewKey)
    - Centro de seguridad de Windows: capacidad de verificar que el estado del Firewall, Antivirus o Centro de seguridad de Windows seleccionado aparece como "Bueno"
    - Asociación de Active Directory: Verificar que el "dominio de inicio de sesión" del usuario coincide con lo especificado en la regla
    - Versión del Sistema Operativo: Verificará que el dispositivo utiliza una versión aceptada (igual y/o superior).

- Postura de seguridad sin necesidad de instalar un agente que incluya, al menos, lo siguiente:
    - Pertenencia a grupo específico de AD.
    - Días y tramos horarios específicos permitidos para acceder.
    - Conexión desde IP pública específica.
    - Conexión desde país específico. Geolocalización.
    - Conexión desde navegador específico.
    - Conexión desde Sistema Operativo específico

La herramienta contará con licencias anuales y soporte directo con el fabricante tipo 24x7. La consola tendrá la posibilidad de gestionarse desde un portal único de administración junto al resto de soluciones incluidas en el lote 1 del expediente.

4.1.2.6. Licencias para la protección de la publicación web y APIs (WAAP)

Se requiere una solución para la protección automatizada de aplicaciones web y API, la misma debe de cumplir con las siguientes características o especificaciones:

- Consola de gestión SaaS y con un único portal de administración junto al resto de soluciones incluidas en el lote 1 del expediente
- Debe darse con un servicio SaaS, evitando el despliegue de nuevos elementos en las instalaciones de VEIASA. Se podrá modificar los registros DNS para realizar el enrutamiento hacia la solución SaaS
- Debe incorporar las siguientes tecnologías de protección:
    - Web Application Protection
    - API Security
    - Bot Prevention
    - Intrusion Prevention (IPS)
    - Prevención de ataques DDoS
    - limite de peticiones http/https
    - Analizar los ficheros que se hayan transferidos en base a su reputación
- La solución debe poder prevenir ciberataques conocidos y desconocidos.
- La implementación debe ser flexible y poderse realizar en nube y on premise
- La prevención de amenazas se realizará en base a motores de inteligencia artificial y no con firmas estáticas.
    - El motor de inteligencia artificial de la solución debe poder llevar a cabo un análisis de riesgos mediante el examen de parámetros como:
        - el perfil del usuario
        - los patrones observados en la sesión del usuario
        - la forma en que otros usuarios interactúan típicamente con la aplicación.
- El motor se debe poder adaptar automáticamente a los cambios de la aplicación al perfilar continuamente el usuario, la aplicación y el contenido.
- La solución deberá incluir un motor de aprendizaje que ayude a disminuir la cantidad de eventos críticos y altos a lo largo del tiempo a medida que aprende el tráfico del sitio y comprende el comportamiento del usuario.
- La solución deberá clasificar cada solicitud y decidir sus posibilidades de ataque a través de un motor de inteligencia artificial

La solución dispondrá de una capacidad para analizar un mínimo de 423 Millones de peticiones HTTP al año.

La herramienta contará con licencias anuales.

4.1.2.7. Licencias de Sandbox

Para proteger los servicios e infraestructura de amenazas provenientes de archivos alojados por los ciudadanos en los repositorios de VEAISA, se requiere la integración a través de API de las aplicaciones utilizadas por VEIASA con una plataforma de inteligencia global donde se analicen dichos archivos. La plataforma dispondrá al menos de las siguientes características:

- Capacidad de detectar archivos maliciosos basados en firmas y emulación de ficheros (sandboxing).
- Motores de prevención de amenazas con capacidad de tomar decisiones en base a inteligencia artificial

Se proporcionarán licencias para realizar al menos 10 mil emulaciones al mes y un millón de consultas por reputación de archivos y contará con soporte directo con el fabricante tipo 24x7

La herramienta contará con licencias anuales.

ENTREGABLES

Con carácter orientativo y con independencia de lo que se pueda solicitar en el contrato basado, el adjudicatario proporcionará mensualmente o cuando sea requerido para ello, los siguientes entregables relacionados con los servicios prestados:

- Informes de Rendimiento y Disponibilidad, Uso de Recursos de Firewall:
  - Estadísticas de CPU, memoria y almacenamiento en los dispositivos.
    - Disponibilidad de Equipos: Tiempos de actividad e inactividad, con análisis de interrupciones y fallas.
    - Rendimiento del Firewall: Datos sobre la cantidad de reglas aplicadas, uso de recursos y estadísticas de tráfico filtrado.
- Informes de Gestión y Operaciones, Estado de Actualizaciones:
  - Registro de firmware y parches instalados, con alertas para actualizaciones pendientes.
  - Registro de modificaciones en las reglas de firewall, incluyendo quién realizó los cambios y cuándo.
- Informes Automatizados para Toma de Decisiones/Recomendaciones para Optimización:
  - Propuestas basadas en análisis históricos para ajustar reglas y políticas de firewall.
  - Simulación de cambios propuestos para predecir posibles impactos en el tráfico de red.
- Informes de Mantenimiento de Hardware:
  - Estado de los Equipos: Diagnósticos periódicos del hardware (CPU, memoria, almacenamiento).

- Identificación de componentes que requieren reemplazo o presentan fallas críticas.
- Registro de eventos de degradación de hardware y acciones correctivas.

- Informe de Garantías y Sustituciones:
  - Detalle de piezas sustituidas bajo garantía o soporte.
  - Fechas de reemplazo y tiempo estimado de vida útil del hardware.
- Informes de Soporte con el Fabricante:
  - Estado del contrato de soporte (vigencia, términos y condiciones).
  - Registro de interacciones con el fabricante (consultas, escalados).
  - Historial de Casos de Soporte
  - Número de incidencias abiertas y resueltas con el fabricante.
  - Tiempos de resolución y cumplimiento de SLA (Service Level Agreement).
  - Resumen de soluciones aplicadas a incidencias reportadas.

4.1.3. ACUERDOS DE NIVEL DE SERVICIO LOTE 1

El adjudicatario se compromete a cumplir con los plazos establecidos en las solicitudes acorde a los palzos establecidos en la tabla de indicadores.

Las penalidades aplicables para el caso de incumplimiento de los ANS mínimos se especifican en la cláusula del Pliego de Cláusulas Administrativas Particulares.

INDICADORES DE CUMPLIMIENTO DE NIVEL DE SERVICIO LOTE 1		
Indicador	Descripción	Objetivo
ANS L1.1	Plazo máximo transcurrido desde la fecha de inicio indicada en el pedido remitido para cada contrato basado por VEIASA hasta la recepción en las instalaciones de VEIASA del equipamiento hardware o la activación de las licencias definidas en el lote 1.	ANS L1.1<= 30 días naturales

4.2. LOTE 2: SERVICIO DE MONITORIZACIÓN Y VIGILANCIA DE LA CIBERSEGURIDAD

4.2.1. Objeto del servicio

El segundo lote contempla la contratación de un servicio para la monitorización y Vigilancia de la seguridad de los sistemas de información de VEIASA y la infraestructura que los soporta , que incluye:

- Servicios de Prevención, Protección, Detección y Respuesta ante incidentes de ciberseguridad en horario continuo (24x7x365).

El servicio demandado se considera un servicio avanzado de ciberseguridad que deberá ser dispensado desde las instalaciones del adjudicatario y gestionado y operado por su personal especialista en modalidad 24x7x365, que mantendrá la dedicación necesaria en cada momento, en función del volumen de alarmas que se pudieran detectar y de su criticidad para VEIASA.

Los licitadores deberán indicar en sus propuestas, que serán objeto de valoracion conforme a lo indicado en el apartado 8 del CR, la organización interna para la prestación de de estos servicios, así como los recursos, medios y herramientas que pondrá a disposición de estos, aportando aquella información que consideren relevante para poder evaluar el grado de madurez del servicio, así como el nivel de especialización y capacidad de los medios y recursos.

4.2.2. Actividades a desarrollar.

Con carácter orientativo, sin ánimo de ser exhaustivo, y con independencia de lo que se pueda solicitar de forma específica en cada contrato basado, el adjudicatario proporcionará los siguientes servicios y desarrollará las actividades descritas en cada uno de ellos.

4.2.2.1. Vigilancia de la Seguridad

4.2.2.1.1. Servicio de Detección en horario continuo (24x7):

El l objeto del servicio será la identificación de cualquier amenaza o violación de la Política de Seguridad de VEIASA que afecte a sus sistemas de información o a las infraestructuras que los soportan y que pueda ser detectada en base al análisis de las alertas y eventos de seguridad detectados a través de un sistema SIEM en el que se integrarán los logs generados en los sistemas de la infraestructura monitorizada descrita en el ANEXO I..

Una vez identificadas las anomalías, el servicio realizará la categorización y contextualización de éstas previa a su comunicación a los servicios de soporte técnico de VEIASA, junto con la recomendación para dar respuesta a las mismas.

El servicio busca incorporar los siguientes beneficios, que deberán ser tenidos en cuenta por los licitadores en sus propuestas:

- Mejorar cuantitativa y cualitativamente el nivel y capacidad de detección de amenazas de seguridad, mediante el análisis de logs de los diferentes sistemas de: protección de seguridad, comunicaciones, de directorio y de información.
- Disponer de un cuadro de mandos sobre el estado de la seguridad y el nivel de amenazas en la organización y el estado de la respuesta a cada una de ellas.
- Acceso a un servicio avanzado que ofrezca un elevado nivel de soporte especializado en la monitorización de la seguridad y gestione las posibles alertas, aportando las recomendaciones adecuadas para acometer su respuesta.
- Automatizar en la medida de lo posible los procesos de detección de amenazas, la comunicación de alertas y la apertura de tickets, mediante las herramientas adecuadas (integración SIEM, XDR, SOAR) que eviten la intervención humana en los procesos, reduciendo así los tiempos de respuesta ante incidentes y posibles errores.
- Contar con un servicio de soporte de CSIRT, que pueda intervenir bajo demanda y de forma diligente y rápida ante incidentes de seguridad, cuya respuesta no pueda ser dispensada por los servicios técnicos de VEIASA.

Además de los aspectos tecnológicos serán objeto de valoracion conforme a lo indicado en el apartado 8 del CR, aquellos aspectos operativos y organizativos, necesarios para la prestación organizada del servicio, así como de los recursos

especializados de soporte y gestión, ofreciendo a VEIASA una solución que cubra el proceso extremo a extremo: desde la ingesta de logs y la detección hasta la comunicación de las alertas, conforme al detalle que se indica en este pliego.

La prestación del servicio deberá incluir todas aquellas tareas, recursos y herramientas necesarias, para su correcta ejecución, proporcionadas por el adjudicatario desde sus instalaciones, entre las que se encuentran como mínimo las siguientes:

- Recopilación y tratamiento de eventos:
    - Velar por la correcta recolección de los eventos de las distintas fuentes, comprobando que se realiza una correcta recepción, filtrado, normalización y almacenamiento de los mismos en la plataforma de correlación.
    - Mantenimiento de la configuración de las políticas de correlación adecuadas para la generación de eventos correlados, creando nuevas políticas o aplicando modificaciones en las existentes.
- Monitorización y evaluación de alarmas.
    - Monitorización de las alertas en tiempo real para identificar qué eventos correlados deben convertirse en alarmas.
    - Evaluación del impacto sobre todas las alarmas generadas.
    - Identificación de la acción o acciones a realizar en base a la criticidad del incidente.
- Definición, adaptación y ejecución de procedimientos para cada alarma, en base a:
    - Tipo de alarma.
    - Criticidad de los activos o servicios afectados.
    - Redes a las que pertenecen.
    - Franja horaria en la que se haya generado la alarma.
    - Existencia o no de vulnerabilidades sobre el activo afectado.
    - En general, en función de cualquier parámetro que puede ser obtenido automáticamente del contenido de la alarma.
- Descarte de alertas, cuando sea considerada como falso positivo tras su correspondiente análisis. Además, se deberá revisar la configuración de las herramientas implicadas para evitar que se vuelva a generar un falso positivo asociado al mismo tipo de actividad identificada y descartada.
- Diseño y mantenimiento de nuevas políticas de correlación o adaptación de las existentes, en base a los requerimientos realizados por VEIASA y/o en base a la evaluación continua de los mecanismos de filtrado y

correlación desplegados, así como del análisis manual de los eventos realizados de forma periódica.

- Comunicación de las alertas al personal designado por VEIASA, así como de las acciones de respuesta o remediación que pudieran corresponder.
- Atención de las solicitudes realizadas por VEIASA, con relación a cualquiera de los aspectos del servicio.

- **SIEM (Security Information and Event Management):**

  El servicio deberá contar como tecnología base un sistema SIEM (Security Information and Event Management), que deberá ser compatible e integrar las diferentes fuentes que VEIASA considere necesarias incluir en el servicio, en el momento del inicio de la ejecución de cada contrato basado, así como otras que durante la vigencia del servicio quisiera incorporar.

  Dispondrá del mayor soporte posible para integrar las fuentes más habituales y/o los medios necesarios para adaptar o integrar fuentes que no estén soportadas de forma estándar.

  El SIEM propuesto por los licitadores, deberá contar con aquellas capacidades, funcionalidades, herramientas y soportes adecuados a la prestación del servicio objeto de esta licitación, conforme a las condiciones del servicio que se indican más adelante.

  Los licitadores deberán realizar el dimensionamiento adecuado del SIEM para soportar la ingesta de los eventos de seguridad que se puedan producir por el conjunto de fuentes que VEIASA incluya en el servicio y que serán inicialmente las siguientes:

  - Protección del puesto de Usuario
  - Firewall
  - Protección del correo
  - Controladores de dominio

  El dimensionamiento del servicio se establecerá en base a ingesta diaria, siendo el requisito mínimo de 100 GB/día

  Se requiere que la solución propuesta por el licitador, esté incluida como producto aprobado o cualificado a fecha de formalización de contrato, en el Catálogo de Productos de Seguridad de las TIC (Catálogo CPSTIC) recogido en la Guía de Seguridad de las TIC CCN-STIC-105 “Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación”, con Categoría ENS “ALTA” para la familia SISTEMAS DE GESTIÓN DE EVENTOS DE SEGURIDAD (SIEM).

- **Detección y Respuesta Avanzada (XDR)**

  Sistema de Detección y Respuesta Avanzada (XDR) que permita:

  - Identificar patrones sospechosos, clasificar y detectar amenazas complejas que podrían pasar desapercibidas con herramientas tradicionales que requieren una mayor intervención humana.
  - Ofrecer informes detallados y recomendaciones automatizadas que los analistas pueden usar directamente
  - Disminuir el tiempo dedicado a la evaluación inicial y al diseño de una respuesta, realizando una priorización automatizada de los incidentes.

- **Custodia de logs:**

  Como parte del servicio, y conforme a las mejores prácticas de seguridad y privacidad, así como a la normativa aplicable, el adjudicatario deberá proporcionar una solución de custodia de logs con las siguiente características:

  - El sistema de custodia de logs deberá estar licenciado y dimensionado para una retención de al menos 13 meses con disponiblidad inmediata a demanda de la información, considerando el total de ingesta diaria propuesta por el licitador. Los licitadores indicarán en sus propuestas las reglas de cálculo para el dimensionamiento del almacenamiento necesario para ello.
  - Para el acceso a los logs, se deberá proveer una consola que permita a VEIASA consultar en cualquier momento la información, disponiendo de una interfaz sencilla, intuitiva y rápida. Esta consola deberá permitir las siguientes capacidades principales:
    - Acceso a información relacionada con volumetría de datos recibidos y almacenados, tipos de eventos agrupados por tecnologías, etc.
    - Informes específicos de cada tecnología de seguridad soportada de forma nativa.
    - Búsquedas avanzadas de cualquier información almacenada aplicando múltiples filtros complejos y permitiendo almacenar dichas consultas para su uso posterior.
    - Enriquecimiento de los datos, facilitando su combinación con información externa.
    - Archivado manual de información mediante la importación de un fichero con logs.
  - Los licitadores deberán incluir en sus ofertas una descripción detallada de la arquitectura de la solución, así como de las funcionalidades y capacidades de la consola de gestión.

4.2.2.1.2. Servicios de Respuesta en horario continuo (24x7):

El constante avance, evolución y sofisticación de las técnicas de ataque y penetración que emplean los ciberdelincuentes, genera un permanente riesgo y tensión en las medidas de seguridad, las cuales en algunas ocasiones pueden resultar insuficientes frente a la tecnología empleada por los criminales cibernéticos que consiguen sobrepasarlas y comprometer los activos.

Por ello VEIASA considera dentro de su estrategia incluir un servicio que le permita estar preparada también ante la probabilidad de padecer un incidente y disponer de la resiliencia adecuada para responder y recuperase del mismo, con el menor esfuerzo, plazo y coste, para dar continuidad a los servicios que presta a los ciudadanos con el mínimo impacto posible.

El objetivo principal del servicio será el de ayudar a los equipos internos de VEIASA a analizar, contener y corregir cualquier incidente de seguridad que se pudiera producir. Se trata de un servicio de alto valor que tendrá una disponibilidad en modalidad 24x7. Deberá intervenir en momentos de crisis, por lo que tendrá que estar prestado por un equipo multidisciplinar formado con personal adiestrado y experimentado en este tipo de intervenciones, disponiendo de las herramientas y medios necesarios para una eficaz actuación.

Las capacidades y características del servicio serán las siguientes:

1. **Equipo de respuesta a incidentes**

- Tal y como se exige en el apartado relativo a la solvencia, se proveerá de un equipo especializado en horario continuo 24x7, para gestionar los incidentes de ciberseguridad y contener el daño, remediar el incidente y restaurar los sistemas afectados, para definir y operar un plan de respuesta a incidentes que establezca las acciones a tomar en caso de un ciberincidente y para realizar análisis forenses y determinar la causa del incidente y el alcance del daño.
- Se proporcionarán los recursos humanos, procedimientos y herramientas para reaccionar rápida y eficazmente ante incidentes de seguridad, gestionando y dando respuesta durante todo el ciclo de vida del Incidente.
- A demanda de VEIASA y previa autorización del Responsable del Contrato, ante incidentes de seguridad de peligrosidad Muy Alta o Crítica (según la catalogación de la guía CCN-STIC 817 del CCN-CERT) que se hubieran materializado, o sobre los que pudiera haber sospecha fundada de su materialización, el adjudicatario ofrecerá un servicio presencial en la instalaciones de VEIASA con desplazamiento del personal especializado del equipo de respuesta, para la aplicación y validación, de las medidas de contención, remediación, erradicación y monitorización post-incidente proporcionadas por el adjudicatario. El coste del desplazamiento esta incluido en el importe ofertado, no pudiendo repercutir VEIASA importe alguno por dicho concepto.
- Dispondrá de un procedimiento operativo maduro que permitirá analizar y responder ante cualquier incidencia de seguridad que se produzca sobre los activos de VEIASA, basado en las siguientes metodologías y marcos de buenas prácticas:

- Metodología aprobada por el CCN-CERT (guía STIC 817) para la gestión y respuesta a incidentes, de acuerdo con el Esquema Nacional de Seguridad (ENS).

- Deberá realizar una correcta categorización de los eventos y clasificación de incidencias o incidentes en base a taxonomía (tipificación) del incidente, la criticidad del activo afectado y la urgencia trasladada por VEIASA, con el objetivo de priorizar y canalizar su gestión a los especialistas y vías de contención/remediaciones correspondientes.
- Tendrá capacidades para aplicar técnicas científicas y analíticas sobre el escenario de un incidente de seguridad, que permitirán identificar, preservar, analizar y presentar los datos que sean válidos, tratados como investigación interna y/o como proceso legal.
- Dispondrá de capacidades para analizar artefactos con distintos niveles de complejidad (estático, dinámico, sandboxing, reversing), tanto de muestras como de alertas de sistemas, que permitan obtener los indicadores de compromiso (IoCs), mecanismos de propagación y propósito de las muestras analizadas.
- Dispondrá de capacidades de investigación digital y forense, incluyendo como mínimo:
  - Triaje inicial, validación del incidente, evidencias preliminares y contextualización del incidente.
  - Extracción de evidencias en sistemas comprometidos y mecanismos facilitados por VEIASA.
  - Análisis de artefactos para identificar sus capacidades (vectores de entrada, técnicas de ofuscación, métodos de propagación, técnicas de exfiltración, etc.), así como obtener indicadores de compromiso (IoCs) y conocer las primeras contramedidas de mitigación.
  - Extracción y custodia de los artefactos forenses de los diferentes elementos involucrados en un incidente mediante procedimientos específicos que harán que las pruebas recogidas sean válidas en incidentes que requieran acciones legales posteriores.
  - Contextualización de amenazas mediante la correlación de evidencias extraídas durante la fase forense para poder evaluar qué primeras acciones de respuesta llevar a cabo.
  - Evaluación del alcance del compromiso (hunting): búsqueda de indicadores de compromiso hallados en etapas anteriores sobre la infraestructura de VEIASA, con el fin de identificar otros activos comprometidos, así como movimientos laterales, escalado de privilegios y otros signos de presencia de actores maliciosos.

  Como parte del equipo mínimo exigido como solvencia, el adjudicatario deberá nombrar un Gestor del Incidente para cada caso, que estará siempre coordinado con el Responsable del Servicio del adjudicatario y que coordinará todo el proceso durante el ciclo de vida de la crisis con VEIASA, así como internamente o con terceras partes que pudieran estar involucradas.
- El adjudicatario Incluirá el soporte necesario a los técnicos y especialista de VEIASA para:
  - La erradicación que consistirá en soporte técnico para la mitigación a largo plazo con el objeto de eliminar el incidente de los sistemas, terminando con

el malware que pueda amenazar la continuidad del negocio, así como con las posibles puertas traseras en los sistemas comprometidos.
- La recuperación, para devolver la red de VEIASA al estado de normalidad anterior al incidente. Este soporte deberá cubrir todos los pasos para restaurar en su caso las copias de seguridad de datos limpias en los sistemas comprometidos, la fortificación y supervisión de los sistemas recién instalados, la implementación de medidas preventivas derivadas de las lecciones aprendidas del incidente que eviten en el futuro se puedan repetir ese mismo tipo de situaciones.
- Aportará capacidades para la revisión periódica de los procedimientos, manuales y herramientas definidos para la gestión de incidentes de seguridad, la preparación y ejecución de un ciberejercicio anual en el entorno de VEIASA, así como el soporte durante la participación de ciberejercicios, públicos o privados, en los que VEIASA decidiera participar.

2. Automatización en la respuesta a incidentes

- El servicio contará con capacidad de Orquestación, Automatización y Respuesta de Seguridad (SOAR) con las siguientes características:
  - Capacidad de Integración:
    - Orquestación con otras herramientas de seguridad (SIEM, cortafuegos, XDR, antivirus) SIEM y con el resto de los elementos que compongan la arquitectura del servicio, que permita automatizar diferentes acciones de respuesta, sin la necesidad de la intervención de un analista, permitiendo una gestión centralizada y coordinada.

  - Notificaciones Automáticas:
    - El sistema emitirá notificaciones de forma automática al equipo de respuesta ante las amenazas detectadas. Para ello, se requiere que se disponga de un sistema, basado principalmente en normalización, categorización y notificación automática de alarmas, que pueda ser adaptado a las necesidades y particularidades de VEIASA.
    - Dicho sistema deberá detectar cualquier alarma generada y en base a los criterios que serán establecidos de forma conjunta, realizará una categorización y notificación a los grupos de operaciones de VEIASA y/o del adjudicatario que deban atender la misma.
    - Los licitadores deberán incluir en sus propuestas un modelo de clasificación de alarmas y matriz de actuación, indicando su tratamiento en función de a quién debe realizarse la notificación y de las acciones que deben realizarse en función de la severidad de la alarma.

  - Capacidades de Mitigación Automática:
    - Como parte fundamental del sistema de orquestación requerido, el mismo debe incorporar la posibilidad de ejecutar acciones de remediación automática que permitan proteger las infraestructuras desde el primer momento en que se genera una alerta de correlación con

objeto de reducir la posibilidad de que llegue a producirse un incidente de seguridad.
    - En este sentido el sistema de orquestación deberá poder actuar automáticamente sobre las principales tecnologías de seguridad del mercado, aumentando la velocidad de respuesta y disminuyendo la necesidad de intervención humana y por tanto la carga operativa del equipo de respuesta, incluyendo: realizar bloqueos de los orígenes identificados como maliciosos, la posibilidad de aplicar parches, bloquear direcciones IP sospechosas o neutralizar amenazas sin intervención humana.
    - Los licitadores indicarán en sus ofertas cuales son las tecnologías de seguridad soportadas, entre las que deberán estar como mínimo los firewalls perimetrales.

- Reglas de configuración y automatización:
    - El adjudicatario deberá indicar las reglas o Playbooks de configuración que tenga disponibles para su sistema de orquestación.
    - El sistema de orquestación permitirá configurar las acciones, en función de la red, usuario afectado, IP o redes afectadas, o cualquier otro valor que pueda ser obtenido de la alarma, para así conseguir un mayor nivel de automatización.
    - El adjudicatario abordará la adaptación de estos a las necesidades particulares de VEIASA y se comprometerá a complementarlos con las reglas que puedan ir siendo precisas durante la vigencia del servicio, aumentando el número de acciones con remediación automática. En este sentido, el adjudicatario deberá realizar las acciones consultivas pertinentes para entender bien el entorno y casos de uso y definir con la colaboración y consenso de VEIASA, la configuración más idónea del sistema de orquestación.

3. Análisis post mortem de los incidentes

- Como parte del ciclo de mejora continua del SGSI de VEIASA y con objeto de contribuir a un incremento de la resiliencia organizacional frente a futuros ciberincidentes, a partir de la información de los incidentes que pudieran haberse materializado, es preciso que el proveedor disponga de un equipo de especialistas en ciberseguridad que, con las herramientas, experiencia y una red de inteligencia adecuadas realice un análisis del incidente que contenga:
    1. La Identificación del Incidente
        - Revisar los eventos y señales que llevaron a detectar el incidente.
        - Confirmar el alcance del ataque (sistemas, datos, usuarios afectados).
        - Determinar la línea temporal exacta del incidente.
    2. Recopilación de Evidencias
        - Reunir datos relevantes, como registros de actividad (logs), reportes de monitoreo, y evidencias digitales.
        - Asegurar que las evidencias sean almacenadas de manera segura y se mantenga su integridad para posibles investigaciones legales.
    3. Análisis del Impacto

- Evaluar las consecuencias del incidente, incluyendo:
- Daños financieros.
- Pérdida o compromiso de datos.
- Afectación a la reputación.
- Interrupciones operativas.
- Determinar si hubo brechas regulatorias o legales.

4. Determinación de la Causa Raíz
   - Identificar cómo se originó el incidente (vulnerabilidades explotadas, errores humanos, fallos de configuración).
   - Analizar si los controles de seguridad existentes fueron suficientes o fallaron.
5. Evaluación de la Respuesta
   Revisar cómo se manejó el incidente en tiempo real:
   - ¿Se siguieron los protocolos establecidos?
   - ¿La comunicación interna y externa fue efectiva?
   - ¿Las medidas tomadas fueron adecuadas para contener y mitigar el incidente?
6. Lecciones Aprendidas
   - Documentar los hallazgos clave.
   - Identificar debilidades en sistemas, procesos o políticas de seguridad.
   - Proponer mejoras concretas basadas en las lecciones aprendidas.
7. Mejora Continua
   - Actualizar los planes de respuesta a incidentes, herramientas de monitoreo y políticas de seguridad.
   - Capacitar al personal en prácticas de seguridad reforzadas.
   - Implementar medidas correctivas, como parches, configuraciones o tecnologías adicionales.
8. Reporte Final
   Elaboración de un informe detallado para los equipos internos, ejecutivos y, si es necesario, las autoridades regulatorias que incluya:
   - Descripción del incidente.
   - Línea temporal.
   - Análisis de impacto.
   - Causas identificadas.
   - Acciones tomadas y mejoras propuestas.

4.2.3. Entregables Lote2

Con independencia de lo que se pueda solicitar en cada contrato basado, y sin ánimo de ser exhaustivos, el adjudicatario proporcionará los siguientes entregables relacionados con los servicios de protección, detección y respuesta a incidentes de seguridad:

- Reglas de configuración y automatización (Playbooks)
- Informe mensual de ciberincidentes, a entregar en la primera semana de cada mes, que incluirá:
  - Número de incidentes de seguridad gestionados.

- Número de incidentes de seguridad por tipo de incidente.
- Número de incidentes de seguridad por sede de VEIASA.
- Número de incidentes de seguridad por nivel potencial de severidad.
- Número de incidentes de seguridad según el impacto o daño causado.
- Número de incidentes de seguridad según el nivel de soporte (TN1, TN2, experto) requerido para su atención
- Propuestas para una mejor gestión de incidentes de seguridad, cuando existan.

- Informe anual de ciberincidentes, a entregar en la primera quincena de cada año natural, que contendrá:
  - Estadística de incidentes de seguridad producidos, con el mismo contenido mínimo que el establecido para el informe mensual de resultados de la plataforma de monitorización.
  - Contexto y tendencias en materia de incidentes de seguridad.
- Informe de ciberincidentes de especial relevancia. Cuando se detecte un incidente de especial riesgo o impacto, además de realizar a la mayor brevedad posible una notificación a la persona responsable del servicio, se le hará entrega en el plazo máximo de 7 días a contar desde el momento de la detección de un informe con el siguiente contenido mínimo:
  - Código o número identificador del incidente.
  - URL, dirección u otro medio que permita consultar el estado del incidente en tiempo real.
  - Teléfono de contacto de las personas o unidades encargadas de la gestión del incidente.
  - Estado del incidente en el momento de la redacción del informe.
  - Explicación a alto nivel del incidente, sus consecuencias potenciales y el impacto producido.
  - Causas u origen del incidente.
  - Medidas adoptadas para hacer frente al incidente.
  - Medidas adoptadas para evitar que el incidente, u otros de similar naturaleza se repita en el futuro.
  - Propuesta de medidas adicionales, cuando sean necesarias.
- Evidencias digitales relacionadas con la gestión de los ciberincidentes.
- Informes de análisis post mortem de los ciberincidentes registrados.

4.2.4. Acuerdos de Nivel de Servicio Lote2

Se analizarán los ANS mensualmente tras el cierre de las actuaciones (provisiones, incidencias, consultas, etc.).

El Responsable del Contrato informará con el detalle del grado de cumplimiento de los distintos ANS al adjudicatario.

El adjudicatario se compromete a cumplir con unos niveles de calidad en los servicios ofrecidos atendiendo a los conceptos descritos en el presente pliego y en las condiciones mínimas que se detallan a continuación en las tablas de indicadores.

Las penalidades aplicables para el caso de incumplimiento de los ANS mínimos, o los ANS mejorados ofertados por el licitador, en su caso, se especifican en el Pliego de Cláusulas Administrativas Particulares.

INDICADORES DE CUMPLIMIENTO DE NIVEL DE SERVICIO		
Indicador	Descripción	Objetivo
ANS L2.1	Plazo máximo transcurrido desde la fecha de inicio indicada en el pedido enviado por VEIASA hasta el inicio de la prestación del servicio con el equipo de trabajo mínimo ofertado.	ANS L2.1<= 14 días naturales.
ANS L2.2	Plazo máximo transcurrido desde que la Dirección del Proyecto autorice la sustitución de un miembro del equipo mínimo de trabajo, hasta la incorporación efectiva del mismo.	ANS L2.2<= 15 días naturales
ANS L2.3	Plazo máximo transcurrido desde que la Dirección del Proyecto solicite la sustitución de algún miembro del equipo mínimo de trabajo, hasta la incorporación efectiva del nuevo miembro que cumpla las exigencias de PPT.	ANS L2.3<= 15 días naturales.
ANS L2.4	Plazo máximo de entrega de informes, documentación y materiales solicitados respecto de las fechas que hubieran sido establecidas en el plan de auditoría / plan de trabajo.	ANS L2.4<= 5 días laborables
ANS L2.5	Plazo máximo de entrega de informes periódicos de cumplimiento de ANS.	ANS L2.5<= 4 días laborables.
ANS L2.6	Plazo máximo transcurrido desde la celebración de una reunión hasta la entrega del acta	ANS L2.6<= 4 días laborables.

Las incidencias de seguridad se priorizarán de acuerdo a su peligrosidad, y se podrán recategorizar por el Responsable del Contrato. La peligrosidad estará determinada según la clasificación de la guía CCN-STIC 817 (Gestión de Ciberincidentes) del CCN-CERT.

A efectos de seguimiento de ANS, se establecen cuatro niveles de peligrosidad, de 0 a 3, siendo 0 el más exigente en cuanto a respuesta, resolución y reparación, y el 3 el menos exigente. Estos niveles se corresponden con los descritos en la guía CCN-STIC 817 de la siguiente forma:

Peligrosidad “0”: niveles de peligrosidad 5 (CRÍTICO) o 4 (MUY ALTO) de CCN-STIC 817.

Peligrosidad “1”: nivel de peligrosidad 3 (ALTO) de CCN-STIC 817.

Peligrosidad “2”: nivel de peligrosidad 2 (MEDIO) de CCN-STIC 817.

Peligrosidad “3”: nivel de peligrosidad 1 (BAJO) de CCN-STIC 817.

Se considerará incumplido cuando se supere el límite del compromiso de Tiempo de Reparación, según se muestra en la tabla siguiente.

GESTIÓN DE CIBERINCIDENTES- INDICADORES DE CUMPLIMIENTO DE NIVEL DE SERVICIO			
Indicador	Peligrosidad	Tiempo de Respuesta	Tiempo de Resolución
ANS L2.6	0	30 minutos	4 horas
ANS L2.7	1	1 hora	6 horas
ANS L2.8	2	2 horas	8 horas
ANS L2.9	3	4 horas	48 horas

Tiempo de Respuesta: Tiempo transcurrido desde la notificación realizada en sistemas (ya sea de manera reactiva por el Responsable del Contrato, o de forma proactiva por el adjudicatario) hasta el envío por parte del adjudicatario de la aceptación de la incidencia indicando el primer diagnóstico en el sistema de tickets en vigor. Se calcula de la siguiente forma:
TiempodeRespuesta=HoradeAceptación−HoradeNotificacióndelaincidencia−ParadasdeReloj

Tiempo de Resolución: Tiempo transcurrido desde que se acepta la incidencia hasta que la incidencia queda resuelta por parte del adjudicatario. Se calcula de la siguiente forma: Tiempoderesolución=Horaderesolución−Horadeaceptación−ParadasdeReloj

ParadasdeReloj :tiempo de respuesta oficial se detiene debido a factores que están fuera del control del equipo de respuesta, como por ejemplo: espera de respuesta de usuario afectado, resolución de restricciones de acceso o de aprobaciones para realizar ciertas acciones.

Existe la posibilidad de reapertura dentro de las 72 horas naturales si el incidente se reproduce. En este caso, el contador de tiempos para el cálculo de los ANS se reactivará desde

el punto en el que se paró, contabilizando el tiempo desde la reapertura hasta la nueva resolución.

4.3. LOTE 3: SERVICIO DE ASISTENCIA TÉCNICA Y DE CUMPLIMIENTO NORMATIVO EN CIBERSEGURIDAD.

4.3.1. Objeto del servicio

El tercer lote contempla la contratación de un servicio de Asistencia Técnica de Ciberseguridad que incluye:

- Servicio de apoyo en tareas de Gobierno Riesgo y Cumplimiento (GRC): actividades de asesoramiento y soporte en el gobierno de la ciberseguridad, gestión de riesgos, cumplimiento legal y normativo (GRC), auditorías internas de cumplimiento ENS, realización de Informes y Cuadros de Mando.
- Auditorías técnicas de seguridad sobre lo sistemas de información de VEIASA y la infraestructura que los soportan.
- Servicios de Formación y Concienciación en Ciberseguridad.

4.3.2. Actividades a desarrollar.

Con carácter orientativo, sin ánimo de ser exhaustivo, y con independencia de lo que se pueda solicitar de forma específica en el contrato basado, el adjudicatario proporcionará los siguientes servicios y desarrollará las actividades descritas en cada uno de ellos.

4.3.2.1. Gobierno, Riesgo y Cumplimiento (GRC)

4.3.2.1.1. Gobierno de la seguridad.

- Asesoramiento en materia de gobierno de la seguridad y elaboración de planes de seguridad orientados a la conformación de estructuras organizativas eficaces en este ámbito y al desarrollo de un cuerpo de normas y procedimientos alineado con las directrices corporativas y con la normativa vigente.
- Asistencia general en materia jurídica, normativa, regulatoria y/o administrativa en aquellos ámbitos con implicaciones en Ciberseguridad.
- Trabajos de soporte para la implantación y mantenimiento de un Sistema de Gestión de la Seguridad de la Información (en adelante, SGSI) adecuado al cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante, ENS), la norma ISO 27001 o cualquier otro esquema de certificación que se determine.
- Diseño, desarrollo y mantenimiento de cuadros de mando específicos, análisis de datos y elaboración de informes en materia de Ciberseguridad como ayuda a la

toma de decisiones al Responsable de Seguridad y al Comité de Seguridad de VEIASA.

- Asesoramiento y soporte al Comité de Seguridad de VEIASA.
- Revisión y actualización del cuerpo normativo de seguridad de VEIASA: política, normas, procedimientos operativos, guías técnicas, procedimientos técnicos y plantillas de informes.
- Apoyo en la adopción de herramientas para la gestión de GRC incluyendo aquellas que se encuentran actualmente en explotación en VEIASA (EasyVista, SGI, JIRA).
- Estudio periódico sobre el Estado de la Seguridad.

4.3.2.1.2. Gestión de activos.

- Soporte en la identificación y valoración de los activos en el ámbito de la Ciberseguridad.
- Colaboración (en los aspectos de la Ciberseguridad) en la elaboración del inventario de activos.
- Coordinación y seguimiento de medidas de protección de activos.

4.3.2.1.3. Gestión del riesgo.

- Análisis y planes de tratamiento de riesgos empleando metodologías y herramientas con suficiente reconocimiento en el sector, como la herramienta Pilar.
- Realización de análisis de impacto en el negocio.
- Elaboración de planes de continuidad y soporte para actividades de simulacro ante incidentes de seguridad.
- Realización de planes de mejora de la seguridad.

4.3.2.1.4. Cumplimiento normativo.

- Trabajos de soporte para el cumplimiento del Esquema Nacional de Seguridad.
- Trabajos de soporte para el cumplimiento de la normativa otras normativas y estándares de seguridad de la información que pudieran ser de aplicación a VEIASA (NIS2, 27001...).
- Soporte en el cumplimiento de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, para garantizar la seguridad de la información de carácter personal y la salvaguarda de los derechos de sus titulares sobre estos datos.
- Soporte al cumplimiento de las obligaciones de registro y suministro de información de seguridad a distintos agentes de referencia (CCN-CERT, Oficina de Apoyo a la Seguridad TIC (OASTIC) de Junta de Andalucía…).

4.3.2.1.5. Auditorías internas de cumplimiento.

- Auditorías internas anuales de cumplimiento en el ámbito del Esquema Nacional de Seguridad.
- Apoyo en la preparación, atención y ejecución de auditorías externas en dicho ámbito.
- Apoyo en la preparación, atención y respuesta a las auditorías o requerimientos de las autoridades de control**.**

4.3.2.1.6. Consultoría y asesoramiento.

- Optimización en el uso de procesos, herramientas, sistemas y metodologías existentes
- Normalización de procesos y procedimientos de seguridad.
- Apoyo legal y/o jurídico y/o administrativo en los proyectos y servicios relacionados con la Ciberseguridad.
- Apoyo en el reporte de incidentes, coordinación y seguimiento de la respuesta a incidentes de ciberseguridad.
- Soporte en la gestión de las posibles denuncias derivadas de un incidente de seguridad.
- Atención de solicitudes de soporte, asesoramiento e información relacionadas con la seguridad.
- Cualquier otra tarea de consultoría relacionada con proyectos y servicios de Ciberseguridad.

4.3.2.2. Auditorías Técnicas de Seguridad

- Análisis de vulnerabilidades: Para identificar y remediar las vulnerabilidades existentes en los sistemas y aplicaciones y evitar que sean explotadas por los atacantes.
- Inspecciones técnicas de seguridad y test de intrusión: Para ayudar a identificar las vulnerabilidades y debilidades de la infraestructura de TI, así como a evaluar la eficacia de las medidas de seguridad existentes.
- Vigilancia digital: Para detectar de forma proactiva amenazas y riesgos antes de que se materialicen en un incidente de seguridad.

  Como actividades más frecuentes, y sin ánimo de ser exhaustivo, se plantean las siguientes:

  - Auditoría de Infraestructura:
    - Análisis de la arquitectura de red:

- Mapeo completo de la red, incluyendo la identificación de todos los dispositivos activos (routers, switches, firewalls, balanceadores de carga, etc.), sus configuraciones y conexiones.
- Evaluación de la segmentación de la red y el flujo de tráfico para identificar posibles puntos débiles en la seguridad.
- Análisis de la seguridad de los dispositivos de red, incluyendo la revisión de configuraciones, firmware, protocolos de enrutamiento y acceso administrativo.

◦ Evaluación de la seguridad perimetral:

- Auditoría exhaustiva de los firewalls, incluyendo la revisión de reglas, políticas de acceso, VPNs, y sistemas de detección y prevención de intrusiones (IDS/IPS).
- Análisis de la configuración de otros dispositivos de seguridad perimetral, como WAFs (Web Application Firewalls), sistemas anti-DDoS y gateways de correo electrónico.
- Pruebas de penetración externas para simular ataques desde fuera de la red e identificar vulnerabilidades explotables.

◦ Evaluación de la seguridad de servidores:

- Revisión de la configuración de seguridad de los servidores, incluyendo la gestión de parches, la configuración de cuentas de usuario y permisos, y la seguridad de los servicios en ejecución.
- Análisis de la seguridad de los sistemas operativos y las aplicaciones instaladas en los servidores.
- Pruebas de penetración internas para evaluar la seguridad de los servidores desde dentro de la red.

◦ Análisis de la gestión de identidades y accesos:

- Evaluación de la seguridad del sistema de gestión de identidades y accesos, incluyendo la autenticación de usuarios, la autorización de acceso a recursos y la gestión de contraseñas.
- Análisis de la seguridad de Active Directory, LDAP u otros servicios de directorio.
- Asesoramiento en la adopción de una solución de gestión de identidades y accesos (IAM) y de su integración con los sistemas y aplicaciones de VEIASA.

◦ Revisión de la gestión de copias de seguridad:

- Evaluación de la estrategia de copias de seguridad, incluyendo la frecuencia, el alcance, el almacenamiento y la recuperación de datos.

- Revisión de la seguridad de las copias de seguridad, incluyendo el cifrado, el control de acceso y la ubicación física.
- Pruebas de restauración para verificar la capacidad de recuperar datos en caso de un incidente.

◦ Análisis de la seguridad de la nube:

- Evaluación de la seguridad de la configuración de la nube, el control de acceso, la seguridad de los datos y el cumplimiento de las mejores prácticas para los servicios en nube que utilice o proporcione VEIASA.

◦ Análisis de vulnerabilidades en aplicaciones web:

- Evaluación de la seguridad de las aplicaciones web utilizando pruebas de penetración, análisis de código fuente estático y dinámico, y revisión de la configuración.
- Identificación de vulnerabilidades comunes como inyección SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) y autenticación rota.

◦ Evaluación de seguridad de APIs:

- Análisis de la seguridad de las APIs (Application Programming Interfaces) utilizadas por las aplicaciones, incluyendo la autenticación, autorización, gestión de errores y protección contra ataques comunes.

◦ Revisión de la seguridad de aplicaciones móviles:

- Evaluación de la seguridad de las aplicaciones móviles en plataformas iOS y Android, incluyendo el análisis de código, la revisión de permisos y la seguridad de los datos almacenados y transmitidos.

◦ Análisis de seguridad de bases de datos:

- Revisión de la configuración de seguridad de las bases de datos, incluyendo el control de acceso, el cifrado de datos y la seguridad de las consultas SQL.

◦ Revisión del código fuente de aplicaciones:

- Análisis estático y dinámico del código fuente de las aplicaciones para identificar vulnerabilidades y errores de desarrollo que podrían comprometer la seguridad.

◦ Evaluación de la seguridad en el desarrollo de software:

- Revisión de las prácticas de seguridad en el ciclo de vida del desarrollo de software (SDLC), incluyendo la seguridad en el diseño, la codificación, las pruebas y el despliegue.

- La evaluación de la seguridad en las líneas de inspección de ITV, las cuales basan su funcionamiento en equipos y sistemas de control industrial, y forman parte del entorno de Tecnología Operacional (OT) de VEIASA, incluyendo:
  - Equipos de control industrial: PLCs, controladores, sensores, actuadores, etc.
  - Redes de comunicación industrial: protocolos de comunicación como Modbus, Profibus, Profinet, Ethernet/IP, etc.
  - Sistemas de monitorización y control (SCADA): software y hardware utilizados para la supervisión y control de los procesos de inspección.
  - Estaciones de trabajo de ingeniería: equipos utilizados para la programación y configuración de los dispositivos OT.
- Seguimiento de la resolución de las vulnerabilidades halladas en las auditorías técnicas.
- Tareas de reauditoría o de auditoría de regresión, a ejecutar pasado un tiempo desde la auditoría principal, y con la finalidad de validar que las acciones correctivas han sido efectivas y se han eliminado las vulnerabilidades detectadas.
- Con carácter general, para todas las actividades relacionadas con las auditorías técnicas (tanto las indicadas arriba a modo de ejemplo como otras que se determinen) y para prevenir que su desarrollo tenga un posible impacto negativo en el funcionamiento de los sistemas de información de VEIASA o de las infraestructuras que los soportan, se aplicarán los siguientes requisitos:
  - Las actividades que sea necesario realizar en cualquiera de los servicios deben ser previamente consensuadas con la Dirección del proyecto. Estas actividades no deben interferir en la operativa diaria de VEIASA, ni comprometer su funcionamiento habitual, reputación o imagen.
  - Para llevar a cabo las actividades requeridas en cada tipo de auditoría técnica de seguridad, el adjudicatario deberá emplear procedimientos y metodologías de trabajo estándar apropiados a cada prueba y podrá apoyarse en el uso de herramientas de seguridad automáticas o semiautomáticas que se complementarán con el empleo de escáneres específicos y revisiones manuales al objetivo de profundizar en los hallazgos y descartar falsos positivos.
  - Dichas herramientas se detallarán en el informe a entregar para cada una de las vulnerabilidades detectadas, para demostrar o evidenciar la existencia de las mismas y su grado de afectación efectiva sobre el sistema auditado, así como demostrar las consecuencias de su materialización. Correrán por cuenta del adjudicatario, tanto los costes de gestión como el licenciamiento de las distintas herramientas comerciales que sea necesario utilizar para la prestación de los servicios.
  - En el citado informe deberá detallarse igualmente la metodología empleada, que necesariamente, incluirá una categorización de vulnerabilidades reconocida internacionalmente (MITRE ATT&CK Framework, OWASP,

OSSTMM, OISSG-ISAAF o equivalentes) así como el escenario y las condiciones de explotación, con el objetivo de poder reproducir las pruebas tras las medidas que se lleven a cabo para mitigar el impacto. También se comunicará el direccionamiento desde el que se lleva a cabo el test, para facilitar la trazabilidad de las auditorias.

- Se le podrá solicitar al adjudicatario la realización de las pruebas necesarias para verificar que se siguen las recomendaciones especificadas en las GUÍAS DE SEGURIDAD DE LAS TIC (CCN-STIC) publicadas por el CCN-CERT.
- En el caso de las auditorías en entornos OT de las estaciones de ITV:
  - La auditoría será realizada por profesionales con experiencia en ciberseguridad industrial.
  - Se deben utilizar herramientas y metodologías de auditoría específicas para entornos OT.
  - La auditoría debe realizarse en colaboración con el personal de VEIASA responsable de la operación y mantenimiento de las líneas de inspección de ITV.
  - Se pondrá especial atención en que el proceso de auditoría no interrumpa la operativa de la estación de ITV más allá de los límites establecidos y consensuados con antelación con la dirección de Proyecto.

4.3.2.3. Formación y Concienciación en el ámbito de la Ciberseguridad.

- Identificación de necesidades y perfiles para la formación y concienciación en materia de confianza y seguridad digital del personal de VEIASA, tanto en la esfera profesional como personal, incluyendo acciones específicas para el personal que desarrolla, gestiona y mantiene los sistemas de información, los puestos de trabajo, servidores e infraestructuras de comunicaciones y de seguridad.
- Prestar soporte integral en el diseño, puesta en marcha, ejecución, seguimiento y evaluación de planes formativos para el desarrollo de competencias y habilidades en materia de ciberseguridad, así como para facilitar la asimilación de cambios culturales en la organización, en distintos niveles, en relación con la adopción de buenas prácticas, la evitación de hábitos de riesgo digital y el fomento de la cultura de ciberseguridad.
- Prestar soporte específico para el diseño, puesta en marcha, ejecución, seguimiento y evaluación de determinadas acciones de concienciación y/o formativas establecidas por la Dirección del proyecto.
- Prestar soporte específico para la elaboración de un plan director de formación y concienciación adaptado a las necesidades de VEIASA.
- Prestar soporte, en coordinación con los proyectos y cauces de comunicación existentes, a las acciones de comunicación necesarias que incentiven la participación en las actividades y la difusión de los contenidos.

- Ofrecer servicio tipo SaaS de plataforma de formación y concienciación.
- Preparación del campus virtual para la formación on-line.
- Calendarización de la formación.
- Apoyo en la certificación de la formación recibida.
- Realización de ejercicios de ciberseguridad que permitan valorar el grado de madurez en materia de ciberseguridad de VEIASA, su capacidad de respuesta ante incidentes, determinar posibles carencias formativas y de concienciación, así como necesidades de mejora tecnológica.

A título orientativo, y sin ánimo de ser exhaustivos, estas actividades podrían agruparse, mediante la combinación de una o varias actividades de un mismo tipo o de distintos tipos, para conformar acciones formativas como las que se muestran a continuación a modo de ejemplo:

- Elaboración planes de acción y de itinerarios
- Materiales de sensibilización: píldoras, vídeos, infografías básicas o avanzadas
- Jornadas/talleres especializados (organización, convocatoria, desarrollo/dinamización).
- Cursos presenciales (5, 10, 20 horas) (diseño/impartición)
- Cursos online (20, 40 horas) (diseño/tutorización)
- MOOC - Masive Open On line Course (diseño/tutorización)
- Seminarios web (1,5 horas) (diseño/impartición)
- La plataforma de formación y concienciación debe de disponer de módulos de formación de una amplia variedad de ámbitos: Secuestro de datos, Redes sociales, Suplantación de identidad, Archivos adjuntos y enlaces peligrosos, Protección de Datos, Seguridad del correo electrónico, Amenazas internas, Malware, Seguridad móvil, Contraseñas, Cumplimiento Normativo, Navegación web, Redes Sociales, Seguridad del dispositivo USB, Trabajar desde casa
- Materiales de autoformación: guías, videopíldoras, podcast...
- Retos gamificados (diseño/impartición).
- Ciberejercicios Table-top: Usados habitualmente para poner a prueba el funcionamiento de los comités de crisis, los protocolos internos de actuación, etc. A partir de un guion previamente elaborado por el adjudicatario, se realizará una simulación de acciones ante una audiencia que deberá tomar decisiones al respecto. Dependiendo de estas decisiones, así como de valores determinados de forma aleatoria, el ciberejercicio tomará un curso u otro, siguiendo el proceso hasta llegar a su finalización.
- Ciberejercicios con Escenario real: acciones reales sobre una audiencia o un sistema o conjunto de sistemas, con objeto de evaluar su nivel de seguridad. El

objetivo puede incluir tanto recursos tecnológicos como organizativos o humanos. Ejemplos típicos de este tipo de ejercicio son la realización de forma controlada de ataques de phishing, los ataques mediante reparto o abandono de pendrives con código malicioso o las suplantaciones de servicio técnico.

4.3.3. Entregables Lote 3

A título orientativo, y sin ánimo de ser exhaustivos, en cada caso aplicable, se efectuará la entrega,según se indique, al menos de la documentación que se indica a continuación:

4.3.3.1. Entregables - Gobierno, Riesgo y Cumplimiento (GRC)

- Políticas, normativas, procedimientos e instrucciones técnicas de seguridad de la información revisadas y actualizadas.
- Inventario de sistemas y activos
- Informes de análisis de riesgo, Informes de aceptación del riesgo residual y planes de mejora de la seguridad para reducción del riesgo resultante.
- Informes de análisis de impacto y planes de continuidad.
- Informes de valoración de las dimensiones de seguridad ENS de los sistemas de información. Informes de declaración de aplicabilidad. Informes de categorización.
- Informes de auditorías de cumplimiento de los sistemas auditados y planes de acciones correctivas.
- Informes de riesgos en el lanzamiento de nuevos proyectos o procedimientos.
- Informes periódicos de actividad (se establecerá la periodicidad al inicio de la ejecución).
- Informes periódicos del cumplimiento de los Acuerdos de Nivel de Servicio (se establecerá la periodicidad al inicio de la ejecución).
- Calendario y planificación de actuaciones
- Actas de las reuniones de seguimiento mantenidas.
- Documentación de soporte al Comité de Seguridad de VEIASA.

4.3.3.2. Entregables – Auditorías Técnicas de Seguridad

Por cada servicio de auditoría técnica adjudicado sobre los sistemas de información de VEIASA y las infraestructuras propias que los soportan:

- Documento de inicio de proyecto con matriz RACI de responsabilidades y plan de proyecto/cronograma con la planificación de los hitos del proyecto. Se especificarán contactos de emergencia para la gestión de posibles incidencias severas durante los trabajos.

- Informe final de las auditorías técnicas. Incluirá, al menos:
- Resumen ejecutivo del resultado de la auditoría.
- Alcance y objetivos.
- Metodología, pruebas realizadas y herramientas utilizadas.
- Resultados obtenidos, identificando los problemas de seguridad encontrados y especificando en qué condiciones se encontraron, con el fin que puedan ser reproducidas (dentro de lo posible) para facilitar su localización y resolución.
- Clasificación de los problemas de seguridad detectados según su nivel de peligrosidad.
- Interpretación y análisis de los resultados.
- Recomendaciones que permitan solucionar de la forma más acertada los problemas de seguridad encontrados.
- Referencias.
- Anexo con los informes generados por las herramientas utilizadas.

4.3.3.3. Entregables - Formación y Concienciación

- Planes de Formación y Concienciación.
- Material de formación y concienciación elaborado.
- Usuarios de acceso a la plataforma online de formación y concienciación.
- Diapositivas empleadas en la impartición de acciones formativas, en formato editable.
- Infografías, píldoras y videotutoriales, en formato editable. Si procedieran de una composición o edición de subcomponentes, se aportarán estos.
- Contenidos de las actividades MOOC, en formato de paquetes SCORM.
- Informes de evaluación de las actividades.
- Informes de propuestas de mejora de la ciberseguridad elaborados a partir de los resultados de las actividades de formación y concienciación realizadas
- Informe general de seguimiento.
- Relación de consultas atendidas.

4.3.3.4. Prestación del Servicio

Los trabajos podrán ser realizados de forma presencial o remota. Particularmente, las siguientes tareas, podrán llevarse a cabo de forma presencial a requerimiento de VEIASA:

- Recogida de información para la elaboración de Análisis de Riesgos

- Reuniones sobre procesos de adecuación al cumplimiento de la normativa de seguridad de la información
- Acompañamieno en procesos de auditoría de certificación en el cumplimiento del Esquema Nacional de Seguridad.
- Acciones de Formación y Concienciación en materia de seguridad de la información.
- Reuniones de preparación las auditorías técnicas de seguridad de los sistemas de información y de las infraestructuras que los soportan así como de presentación de sus resultados.
- Reuniones de seguimiento de los trabajos

El horario de prestación de estos servicios cubrirá al menos el horario de trabajo habitual de VEIASA para OOCC.

Los horarios de realización de las auditorías técnicas de seguridad se planificarán con la debida antelación, con objeto de evitar interferferencias con la dinámica de trabajo de VEIASA o minimizar los posibles problemas de rendimiento que estas pruebas de seguridad puedan ocasionar. En consecuencia, normalmente, estas auditorías técnicas se llevarán a cabo fuera del horario laboral de VEIASA en el horario acordado entre el adjudicatario y el Responsable del Contrato para cada caso particular.

4.3.4. Acuerdos de Nivel de Servicio Lote 3

El adjudicatario se compromete a cumplir con unos niveles de calidad en los servicios ofrecidos atendiendo a los conceptos descritos en el presente pliego y en las condiciones mínimas que se detallan a continuación en la tabla de indicadores:

INDICADORES DE CUMPLIMIENTO DE NIVEL DE SERVICIO			
Tipo de indicador	Indicador	Descripción	Objetivo
Equipo de trabajo	ANS L3.1	Plazo máximo transcurrido desde la fecha de inicio indicada en el pedido enviado por VEIASA hasta el inicio de la prestación del servicio con el equipo de trabajo mínimo ofertado.	ANS L3.1<= 14 días naturales.
	ANS L3.2	Plazo máximo transcurrido desde que la Dirección del Proyecto autorice la sustitución de un miembro del equipo mínimo de trabajo, hasta la incorporación efectiva del mismo.	ANS L3.2<= 15 días naturales
	ANS L3.3	Plazo máximo transcurrido desde que la Dirección del Proyecto solicite la sustitución de algún miembro del equipo mínimo de trabajo, hasta la incorporación efectiva del nuevo miembro que cumpla las exigencias de PPT.	ANS L3.3<= 15 días naturales.
	ANS L3.4	Plazo máximo de entrega de informes, documentación y materiales solicitados respecto de las fechas que hubieran sido establecidas en el plan de auditoría / plan de trabajo.	ANS L3.4<= 5 días laborables
	ANS L3.5	Plazo máximo de entrega de informes periódicos de cumplimiento de ANS.	ANS L3.5<= 4 días laborables.
	ANS L3.6	Plazo máximo transcurrido desde la celebración de una reunión hasta la entrega del acta	ANS L3.6<= 4 días laborables.

Se analizarán los ANS mensualmente tras el cierre de las actuaciones (provisiones, incidencias, consultas, etc.).

El Responsable del Contrato informará con el detalle del grado de cumplimiento de los distintos ANS al adjudicatario.

Las penalidades aplicables para el caso de incumplimiento de los ANS mínimos, o los ANS mejorados ofertados por el licitador, se especifican en la cláusula del Pliego de Cláusulas Administrativas Particulares.

5. MODO, FASES Y SEGUIMIENTO DE LA PRESTACIÓN DE LOS SERVICIOS.

- Para la planificación de las tareas se realizarán reuniones de trabajo con la periodicidad que se determine, en las que se revisará el estado de las tareas en curso y se determinarán las prioridades, tareas a abordar y plazos de realización. Igualmente, se estimarán y planificarán periódicamente los esfuerzos necesarios de los perfiles.
- Periódicamente, se realizarán reuniones de seguimiento entre la Dirección de Proyecto, por parte de VEIASA, y la Jefatura de Proyecto, por parte de la persona adjudicataria, al objeto de revisar el grado de cumplimiento de los objetivos, hitos y la validación de las programaciones de actividades realizadas, así como los informes de evaluación de ANS. De estas reuniones de seguimiento se levantarán actas por parte de la Jefatura de Proyecto, que deberán ser aprobadas por la Dirección de Proyecto. Se establecerá flujo de aprobación para este proceso.
- Para la gestión y el seguimiento de los trabajos, sin perjuicio de otras que se indiquen, la persona adjudicataria utilizará la herramienta de gestión de proyectos que se indique por parte de la Dirección del Proyecto. Con esta herramienta se realizará el seguimiento de las tareas y los servicios y la medición de los indicadores que se hayan definido.
- Con objeto de facilitar y evidenciar el cumplimiento de los servicios prestados, el adjudicatario presentará, cuando sea requerido, los siguientes entregables:
  - Calendario y planificación de actuaciones.
  - Actas de las reuniones de seguimiento mantenidas.
  - Informes periódicos de actividad (se establecerá la periodicidad al inicio de la ejecución).
  - Informes periódicos del cumplimiento de los Acuerdos de Nivel de Servicio (se establecerá la periodicidad al inicio de la ejecución).
  - En general, documentos resultantes de las tareas realizadas.

6. ORGANIZACIÓN DEL TRABAJO

Es un objetivo prioritario de VEIASA asegurar la calidad de los trabajos realizados, y que han sido objeto de valoracion según el apartado 8 del CR, por lo que las empresas que resulten adjudicatarias implantarán metodologías y mecanismos organizativos internos para la prestación del servicio con el fin de asegurar la correcta ejecución de los trabajos, en los plazos estipulados en el programa de trabajo, la coordinación interna, la resolución de los problemas que pudieran surgir durante el desarrollo de los trabajos y la calidad del producto final entregado, así como los mecanismos y herramientas de interlocución con VEIASA.

Será necesario que en esta organización específica prevista para el desarrollo del proyecto cada función quede perfectamente identificada y tenga asignada una persona responsable de su cumplimiento.

6.1. FUNCIONES Y RESPONSABILIDADES

Para el control, dirección y ejecución de los contratos se establecerán de forma concreta las siguientes figuras, sin perjuicio de que el adjudicatario quiera ofertar otras adicionales para asegurar la calidad de los trabajos y conseguir una mejor prestación del servicio:

• Responsable del Contrato y Dirección del proyecto.

• Jefe de Proyecto.

• Equipo de proyecto.

Las funciones y responsabilidades de estas figuras serán las siguientes:

6.1.1. Responsable del contrato y dirección del proyecto

El Responsable del Contrato será una persona designada por VEIASA, siendo sus funciones y responsabilidades:

- Dirigir, supervisar y coordinar la realización y desarrollo de los trabajos.
- Aprobar el programa o planificación de realización de los trabajos.
- Velar por el nivel de calidad de los trabajos.
- Participar y coordinar las entrevistas o reuniones entre usuarios y técnicos involucrados en el proyecto.
- Decidir sobre la aceptación de las modificaciones técnicas propuestas por la Jefatura de Proyecto a lo largo del desarrollo de los trabajos.
- Asegurar el seguimiento del Programa de realización de los trabajos.
- Hacer cumplir las normas de funcionamiento y las condiciones estipuladas en este Documento.

- Autorizar cualquier alteración de la metodología empleada, tanto en los productos finales, como en la realización de las fases, módulos, actividades y tareas.
- Aprobar la participación en el proyecto de las personas del equipo de trabajo aportado por la empresa adjudicataria, así como sugerir o exigir la sustitución de alguna o algunas de las personas miembros del equipo (tanto del Jefe de Proyecto como del equipo del Proyecto) si a su juicio su participación en el mismo dificulta o pone en peligro la calidad o la realización de los trabajos.
- Aprobar la composición del equipo de trabajo aportado por la empresa adjudicataria. El Jefe de Proyecto tiene la obligación de mantenerle informado sobre cualquier modificación que se pueda producir en el equipo de trabajo, que también requerirán aprobación expresa.
- Aprobar los resultados parciales y totales de la realización del proyecto; a estos efectos deberá recibir y analizar los resultados y documentación elaborados a la finalización de cada etapa, pudiendo introducir las modificaciones o correcciones oportunas antes del comienzo de las siguientes, requiriéndose su aprobación final.

El Responsable del Contrato podrá delegar funciones de operación y seguimiento en una persona o grupo de personas designadas, que conformarán la Dirección del proyecto.

6.1.2. Jefe de Proyecto

Es una persona aportada por la empresa adjudicataria, siendo su responsabilidad la ejecución de los trabajos. Además, tendrá como objetivos específicos los siguientes:

- Organizar la ejecución del proyecto de acuerdo con el Programa de realización de los trabajos y poner en práctica las instrucciones de la Dirección del proyecto.
- Ostentar la representación del equipo técnico contratado en sus relaciones con VEIASA en lo referente a la ejecución de los trabajos.
- Proponer a la Dirección del proyecto las modificaciones que estime necesarias, surgidas durante el desarrollo de los trabajos.
- Asegurar el nivel de calidad de los trabajos.
- Presentar a la Dirección del proyecto, para su aprobación, los resultados parciales y totales de la realización del proyecto.
- Comunicar a la Dirección del proyecto cualquier riesgo identificado en las planificaciones.
- Servir de interlocutor con otros equipos de trabajo y de coordinación de los mismos cuando tengan que intervenir en actividades planificadas.
- Informar periódicamente a la Dirección del proyecto sobre el estado del servicio, avance de trabajos en curso, cumplimiento de hitos y riesgos en el cumplimiento de los hitos planificados.
- Informar a la Dirección del proyecto sobre cualquier modificación que se pueda producir en el equipo de trabajo, las cuales no podrán llevarse a efecto sin la aprobación expresa de la Dirección del proyecto.
- Proponer a la Dirección del proyecto el redimensionamiento del equipo de trabajo para cumplir con la demanda de servicios existente en cada momento.

6.1.3. Equipo de Proyecto

Debido a que las actuaciones, metodologías y tecnologías en el ámbito de las TIC pueden variar a lo largo de la duración del acuerdo marco, no es posible determinar con exactitud la relación de perfiles especializados que les darían cobertura y las necesidades específicas para cada uno de ellos. No obstante, se indica como referencia que los perfiles susceptibles de ser requeridos son aquellos referenciados en el acuerdo técnico CWA 16458-1:2018 “European ICT professionals role profiles - Part 1: 30 ICT profiles” cuyas funciones y tareas están descritas en dicho acuerdo.

En el apartado del CR correspondiente a la solvencia técnica y profesional, se indica el equipo mínimo de trabajo, así cómo su experiencia, titulación y certificaciones exigidas para cada uno de los miembros de dicho equipo mínimo. Estos extremos se acreditarán según lo expecificado en el CR.

La composición mínima del equipo de proyecto se relaciona en la siguiente tabla:

Lote	Perfil	Recursos
Lote 2	Gestor de Ciberseguridad que actuará también como Jefe de Proyecto	1
	Especialistas en Ciberseguridad	4
	Especialistas Técnicos	4
Lote 3	Gestor de Ciberseguridad que actuará también como Jefe de Proyecto	1
	Especialistas en Ciberseguridad	1
	Especialistas Técnicos	1

El gestor de ciberseguridad puede ser el mismo perfil para ambos lotes.

Si, a juicio de VEIASA, alguno de los recursos propuestos no ejecutara los servicios descritos conforme a las exigencias del presente PPT, deberá ser sustituido adecuadamente en un plazo máximo de 15 días naturales, sin que esto afecte ni a la planificación de trabajos prevista ni a la estimación de costes del proyecto.

De forma específica se requiere que el personal del equipo de trabajo mínimo indicado tenga la **experiencia mínima , titulación y certificaciones de seguridad** que se establecen en el cuadro resumen del Pliego de Cláusulas Administrativas Particulares.

6.2. OTRAS OBLIGACIONES DEL CONTRATISTA

- Elaborar informes, presentaciones, guías, manuales u otra documentación técnica relacionada con el objeto de la prestación.
- Mantener durante el periodo que dure la prestación, un alto nivel de conocimiento a través del desarrollo de acciones de prospectiva, así como una constante actualización en tendencias, innovaciones y materias relacionadas con el objeto de la prestación en el ámbito nacional e internacional.
- Reportar periódicamente a la Dirección de los trabajos sobre el desarrollo y evolución de la actividad desarrollada.
- Asistir a reuniones o eventos en los que la Dirección de los trabajos necesite de los servicios de asistencia técnica que son objeto de la presente contratación.
- Adoptar en el día a día los mecanismos de funcionamiento y herramientas de coordinación que la Dirección de los trabajos determine a tal efecto.
- Realizar una Transferencia de Conocimientos completa, entregando toda la documentación técnica, manuales de usuario, configuraciones específicas y cualquier otro material relevante, además de realizar sesiones de capacitación en base a un plan de transferencia detallado, definiendo un periodo de transición para ello.
- Garantizar el flujo constante de información de la actividad con el equipo de trabajo de la Dirección de los trabajos.

7. CONDICIONES DE LA PRESTACIÓN DEL SERVICIO

7.1. ORIENTACIÓN A SERVICIO

Para la prestación del servicio objeto del presente acuerdo marco, las empresas licitadoras deberán ofrecer un servicio integral que permita disponer de los recursos técnicos necesarios en cada momento para poder dar respuesta, con los niveles de calidad requeridos y dentro de los plazos exigidos en el correspondiente acuerdo nivel de servicio.

Las empresas deberán dirigir sus proposiciones técnicas hacia un enfoque orientado al servicio y no a los recursos, debiendo concretar en sus respectivas ofertas el nivel de flexibilidad ofrecido en cuanto a composición del equipo de trabajo, ubicación del mismo (preferentemente en las instalaciones de la empresa adjudicataria) y disponibilidad de equipos expertos para absorber trabajos específicos y/o puntas de trabajo, etc.

7.2. COMPOSICIÓN Y CAMBIOS EN EL EQUIPO DE TRABAJO

El equipo de trabajo deberá aportar conocimiento del negocio de las distintas áreas funcionales de VEIASA que se requieran, de cara a ofrecer valor añadido para la integración o

la aparición de nuevas necesidades.

El equipo de trabajo debe asumir el procedimiento de trabajo de VEIASA y cumplir con las especificaciones marcadas por la misma en las condiciones del contrato.

El equipo de trabajo exigido, deberá estar plenamente incorporado al inicio del contrato y durante la vigencia del mismo. La autorización de cambios puntuales en la composición del equipo mínimo requerirá de las siguientes condiciones:

- Justificación por escrito, detallada y suficiente, explicativa del motivo del cambio. Se presentará a la Dirección del proyecto.
- Presentación de posibles candidatos para el perfil cuya cualificación técnica sea igual o superior al de la persona que se pretende sustituir, donde el adjudicatario deberá informar por escrito a la Dirección del proyecto acerca de la formación, conocimientos, certificaciones y experiencia de los nuevos recursos.
- Aceptación por la Dirección del proyecto del candidato propuesto.

Tras el análisis del informe por parte de la Dirección del proyecto, ésta lo autorizará si así lo considera y con las condiciones o limitaciones que considere convenientes. Los posibles inconvenientes de adaptación al entorno de trabajo y al desarrollo del servicio debido a sustituciones de sus componentes del equipo mínimo, deberán subsanarse mediante periodos de solapamiento, sin coste adicional para VEISA durante el tiempo necesario. El plazo de solapamiento mínimo entre el perfil entrante y el saliente será mínimo de 5 días.

Queda establecido que la gestión del equipo de trabajo del adjudicatario del contrato basado es de su única responsabilidad. No obstante, el adjudicatario deberá garantizar que dispone de los mecanismos adecuados para que la rotación no planificada del equipo de trabajo que ejecuta los servicios en todos los entornos no impacte en la pérdida no controlada de conocimiento y en los niveles de calidad del servicio, imagen y la dedicación adicional de personal de VEIASA que una rotación inadecuada lleva asociada.

Por rotación planificada se entiende aquella comunicada a VEIASA con al menos un mes de antelación a que se produzca la salida.

Durante la ejecución del contrato, VEIASA podrá verificar en cualquier momento la adecuación a los requerimientos que se hayan solicitado para cada componente del equipo mínimo de trabajo (según los perfiles de titulación académica, formación adicional y actividad profesional). La falsedad en el nivel de conocimientos técnicos y experiencia de alguno de los componentes del equipo adscrito a la ejecución de los trabajos facultará a VEIASA a requerir la sustitución de dicho recurso.

7.3. FORMACIÓN CONTINUA

El adjudicatario se compromete a mantener el nivel de conocimientos y cualificación del equipo de trabajo durante el periodo de ejecución del contrato, mediante la formación continua en las tecnologías que forman parte del proyecto u otras que estén previstas implantar y que VEIASA informe con, al menos, un mes de antelación.

7.4. HORARIO DE LA PRESTACIÓN DEL SERVICIO

Los calendarios y horarios que el adjudicatario deberá cubrir se especifican en las actividades a realizar en cada lote para cada contrato basado

7.5. LUGAR DE REALIZACIÓN Y RECURSOS NECESARIOS

El equipo de trabajo realizará sus tareas de forma habitual de manera remota desde las instalaciones del adjudicatario, salvo determinadas tareas que se especifican en las actividades a desarrollar de cada lote.
Es responsabilidad de la empresa contratista facilitar a sus trabajadores los medios materiales necesarios para llevar a cabo su trabajo.

No obstante lo anterior, las actividades a desarrollar vinculadas a los servicios profesionales asociados al contrato que pudieran requerir el desplazamiento a cualquier punto de la Comunidad Autónoma de Andalucía en la que VEIASA disponga de instalaciones, tanto para su realización como para la presentación de resultados, sin que ello suponga un coste adicional para VEIASA.

7.6. HERRAMIENTAS DE GESTIÓN DEL SERVICIO Y DE ATENCIÓN A PERSONAS USUARIAS

Salvo que la Dirección del proyecto y el proveedor acuerden lo contrario, la empresa proveedora de los servicios utilizará el software de gestión del servicio que le indique aquel para el almacenamiento y gestión de los datos necesarios para el seguimiento del servicio en cada contrato basado.

El acceso de las personas técnicas del equipo de proyecto de la empresa adjudicataria será autorizado por VEIASA.

El modo de acceso de este personal será tal que garantice la seguridad de operación y explotación del sistema, así como el objetivo de almacenar y gestionar las solicitudes de servicio e incidencias que se produzca durante la ejecución del contrato.

7.7. PROPIEDAD INTELECTUAL DE LOS TRABAJOS

Todos los estudios y documentos, así como los productos y subproductos elaborados por el contratista como consecuencia de la ejecución de los contratos basados en el presente acuerdo marco serán propiedad de VEIASA, quien podrá reproducirlos, publicarlos y divulgarlos, total o parcialmente, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos.

El adjudicatario renunciará expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del presente contrato pudiera corresponderle,

y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa de VEIASA, específicamente todos los derechos de
explotación y titularidad de las aplicaciones informáticas y programas de ordenador desarrollados al amparo de esta contratación, corresponden únicamente a VEIASA.

La presente cláusula no será de aplicación a los productos y herramientas preexistentes empleados para la ejecución del contrato protegidos por derechos industriales o de propiedad intelectual.

7.8. METODOLOGÍA

Dadas las especiales características de este trabajo, los procesos y las actividades que indica la metodología se adaptarán al mismo con el objeto de conseguir la mayor eficacia en su desarrollo. Las empresas oferentes indicarán en el documento técnico que presenten la adecuación metodológica al proyecto que proponen.

La Dirección del proyecto aprobará al comienzo de cada contrato basado las directrices metodológicas e interpretará de igual modo las posibles dudas que sobre su aplicación puedan surgir a lo largo de la ejecución del proyecto.

7.9. SEGURIDAD

Las proposiciones deberán garantizar el cumplimiento de los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información que constituyen el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

En concreto, se deberá asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que son objeto de la presente contratación. A tal fin, los licitadores deberán disponer y aportar con la presentación de la oferta en el sobre 3, la certificación en vigor en el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) para nivel MEDIO o ALTO.

Deberá también tenerse en cuenta lo dispuesto en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio) y en su desarrollo a partir de la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía y normativa asociada.

Se atenderá también a la normativa interna de VEIASA en materia de Seguridad TIC.

Además, se deberá atender a las mejores prácticas sobre seguridad recogidas en las series de documentos CCN-STIC (Centro Criptológico Nacional - Seguridad de las Tecnologías de Información y Comunicaciones), disponibles en la web del CERT del Centro Criptológico Nacional (http://www.ccncert.cni.es/), así como a las guías y procedimientos aplicables elaborados por la Unidad de Seguridad TIC Corporativa de la Junta de Andalucía.

7.10. USO DE INFRAESTRUCTURAS TIC Y HERRAMIENTAS CORPORATIVAS

Se tendrán en cuenta todas las infraestructuras TIC (sistemas de información, tecnologías, frameworks, librerías software, etc.) que en la junta de Andalucía tenga la consideración de corporativas u horizontales y sean susceptibles de su utilización.

NAVAS MORA JOSE LUIS - 27302346N

Firmado digitalmente por NAVAS MORA JOSE LUIS - 27302346N
Fecha: 2025.08.01 14:35:12 +02'00'

En Sevilla a fecha de firma digital.
Fdo: José Luis Navas Mora
Responsable de Seguridad de la Información

8. ANEXO I. SISTEMAS PREEXISTENTES, ARQUITECTURA Y NIVELES DE CRITICIDAD.

ANEXO I. SISTEMAS PREEXISTENTES, ARQUITECTURA Y NIVELES DE CRITICIDAD.

CONFIDENCIAL

Este anexo será remitido a los licitadores, previa solicitud al correo licitaciones@veiasa.es, debiendo aportar en dicha solicitud la Cláusula de Confidencialidad (Anexo II del PPT), debidamente cumplimentada, firmada y sellada por representante con poder suficiente (debiendo acreditarse igualmente el poder de representación).

9. ANEXO II- CLÁUSULA DE CONFIDENCIALIDAD

ANEXO II- CLÁUSULA DE CONFIDENCIALIDAD

Don _____, con D.N.I. nº._____, actuando en nombre y representación de _____ (en lo sucesivo, la EMPRESA), entidad con domicilio en _____ y C.I.F. _____, con motivo de la licitación con nº de Expediente CF050-23-051, PRESTACIÓN DE SERVICIOS DE CIBERSEGURIDAD GESTIONADA.

EXPONE Y ACEPTA QUE

1. Se compromete a guardar la máxima reserva y secreto sobre la información clasificada como confidencial. Se considerará Información Confidencial cualquier información de VERIFICACIONES INDUSTRIALES DE ANDALUCÍA, S.A. (en adelante, VEIASA) relacionada con la licitación del procedimiento de contratación de la PRESTACIÓN DE SERVICIOS DE CIBERSEGURIDAD GESTIONADA, Expediente: CF050-23-051, a la que EL LICITADOR accede en el marco de la referida licitación, y en particular la información contenida en el Pliego de Prescripciones Técnicas, Pliego de Condiciones Administrativas Particulares y Cuadro Resumen aplicables a la referida licitación que se entrega en este acto a EL LICITADOR.

2. EL LICITADOR únicamente podrá utilizar dicha Información Confidencial con las finalidades relacionadas directamente con la preparación de su oferta para participar en la licitación del procedimiento de contratación referido anteriormente, y se obliga a no utilizar dicha Información Confidencial para cualquier finalidad distinta de la anterior.

3. EL LICITADOR se compromete a no divulgar dicha Información Confidencial, así como a no publicarla ni de cualquier otro modo, bien directamente bien a través de terceras personas o empresas, ponerla a disposición de terceros sin el previo consentimiento por escrito de VEIASA.

4. De igual modo, EL LICITADOR se compromete, tras la finalización del procedimiento de licitación o, en su caso, la extinción de la relación contractual con VEIASA a no conservar copia alguna de la Información Confidencial, en cualquier tipo de soporte.

5. EL LICITADOR informará a su personal, colaboradores y subcontratistas, en su caso, de las obligaciones establecidas en el

presente compromiso sobre confidencialidad. EL LICITADOR realizará cuantas advertencias y suscribirá cuantos documentos sean necesarios con su personal y colaboradores, con el fin de asegurar el cumplimiento de tales obligaciones.

6. Las obligaciones de confidencialidad establecidas en el presente compromiso tendrán una duración indefinida, manteniéndose en vigor con posterioridad a la finalización del procedimiento de licitación o, en su caso, de la extinción de la relación entre VEIASA y EL LICITADOR.

7. VEIASA podrá, por sí mismo o por medio de terceros, inspeccionar el cumplimiento por parte de EL LICITADOR de las estipulaciones reguladas en virtud del presente compromiso, incluso, en las propias instalaciones de EL LICITADOR.

8. El incumplimiento por parte de EL LICITADOR de cualquiera de las obligaciones establecidas en el presente compromiso, dará derecho a VEIASA a percibir una indemnización por los daños y perjuicios que le sean causados.

9. Asimismo, dicho incumplimiento generará, en su caso, el derecho de VEIASA a dar por resuelto el Contrato que pudiera serle adjudicado en el marco del referido procedimiento de licitación, sin corresponder indemnización alguna a favor de EL LICITADOR por tal concepto.

Y para que así conste, y en prueba de conformidad y aceptación al contenido del presente escrito, quien comparece lo firma, en ……., a……de ……..de……...

(Sello de la empresa)

Fdo.: